REMARKS

Applicants have thoroughly considered the Examiner's remarks in the November 10, 2008 Office action. This Amendment E amends claims 1, 15, 22, and 35 and cancels claims 12 and 13. Claims 1-10, 15, 19, 20, 22, 23, 30, and 32-38 are thus presented in the application for further examination. Reconsideration of the application as amended and in view of the following remarks is respectfully requested.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-10, 12, 13, 15, 19, 20, 23, 30, 32 and 34 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Venkataramappa (U.S. Pub. App. 2003/0188193, hereinafter Venkataramappa) in view of Zhang et al. (U.S. Pat. No. 7,036,142, hereinafter Zhang) further in view of Lutz (U.S. Pub. No. 2003/0204579, hereinafter Lutz). Applicants respectfully disagree.

Lutz teaches a method of for providing network management services. (Abstract). The user enters a start page of the server providing the network management services. (Page 4, [0040]). Applicants disagree with the Examiner's assertion on page 4 of the action that paragraph 36 of Lutz teaches "storing first data on the client in response to the received first request, said first data identifying the first service wherein the authentication of the user by the first service is optional" and "allowing the user to access the first service without authenticating" as recited in claim 1.

First, with respect to the optional authentication, Lutz teaches **that at the point the user confirms the request for network management servers, the user may be optionally authenticated for personalized services.** (FIG. 8; page 4, [0043]; page 7, [0074]). However, before the network management service selected by the user is executed, the user must enter "**network specific authentication information** which is required to perform the network management service." (Page 4, [0043]; page 7, [0074]). Therefore, Lutz, alone or in combination with the other cited art, fails to teach or disclose "allowing the user to access the first service without authenticating" as recited in claim 1.

With respect to "storing first data on the client in response to the received first request, said first data identifying the first service", Lutz teaches sending an analyzer selection page to the user. (Page 4, [0041]). The analyzer selection page is a web page which enables the user to "pre-select one of several analyzers to be used in the subsequent service management carried out

by the service provider." (Page 4, [0042]). Next, the user selects a specific type of analyzer from the web page and sends the analyzer selection to the server. (FIG. 8, page 7, [0074]). **In other words the client does not store information identifying the requested service, instead the client sends information identifying the requested service to the service provider.**

Claim 22

In contrast, claim 22 as amended recites:

> a first network server coupled to a data communication network, said first network server being configured to provide a first service to a user via a client also coupled to the data communication network;
>
> a second network server coupled to the data communication network, said second network server being configured to provide a second service to the user via the client;
>
> a central server coupled to the data communication network, said central server being configured to receive a first request from the first network server to provide the first service to the user and a second request from the second network server to provide the second service to the user;
>
> said first network server being configured to direct the first request to the central server, said **central server further being configured to generate and store first data on the client in response to receiving the first request, said first data identifying the first service** wherein authentication of the user by the first service is optional and wherein the user is not authenticated for the first service and not authenticated for the second service, **said first service allowing the user to access the first service without authenticating the user during which the user continues to be unauthenticated for the first service and unauthenticated for the second service;**
>
> said second network server being configured to direct the second request to the central server, said second service requires authentication of the user;
>
> wherein, in response to the received second request, the central server is configured to allow the user access to the second service **wherein the user is authenticated for the second service in response to the received second request**; and
>
> wherein, **in response to authentication of the user by the second request, the central server is configured to authenticate the user for the first service identified in the stored first data**.

As explained above, Lutz teaches only that personalization authentication is optional and that before the network management service selected by the user is executed, the user must enter "**network specific authentication information** which is required to perform the network management service." And, even if Lutz discloses authentication to a client is optional, none of

the cited references, either separately or in combination, disclose "**storing first data on the client in response to the received first request, said first data identifying the first service**" and "**in response to the authentication of the user by the second request, the user is authenticated for the first service indentified in the stored first data**" as recited in the claim 22. For example, Lutz may disclose that a list of services is provided to the user, but Lutz fails to teach storing first data identifying the first requested service as recited in claim 22.

Writing for the Supreme Court, Justice Anthony Kennedy observed that a patent claim is invalid for obviousness when the invention combines familiar elements according to known methods to produce no more than predictable results. *KSR International Co. v. Teleflex, Inc.* U.S., No. 04-1350, 4/30/07. However, in this rejection, neither the **element** of **storing first data on the client in response to the received first request ... wherein the user is not authenticated for the first service and not authenticated for the second service when the first data is stored**" nor the **result** of "**in response to the authentication of the user by the second request, the user is authenticated for the first service identified in the stored first data**" is found in the combined art.

For at least these reasons, Applicants submit that cited references, alone or in combination, do not teach or make obvious each and every element of claim 22. As such, the rejection of claim 22 under 35 U.S.C. § 103(a) should be removed. Claim 35 has been amended to include similar subject matter as claim 22 and is allowable for at least the same reasons as claim 22. Claims 23 and 36-38 depend from claims 22 and 35. respectively, and are allowable for at least the same reasons as claims 22 and 35

Claim 15

Claim 15, as amended, recites:

receiving a first request from the first network server to provide the first service to the user wherein the first service requires authentication of the user;

authenticating the user for the first service in response to the received first request;

allowing the user access to the first service in response to the received first request **wherein an authentication ticket and profile information associated with the user is communicated to the first service**;

storing first data on the client in response to allowing the user access to the first service, said first data identifying a first policy group associated with the first

service, **said first policy group having a shared set of business rules to restrict authentication of a user across different domains**;

receiving a second request from the second network server to provide the second service to the user wherein authentication of the user by the second service is optional and wherein the user is not authenticated for the second service;

if the second service is associated with the first policy group identified by the stored first data, allowing the user access to the second service in response to the received second request wherein the user is authenticated for the second service in response to the received second request **and wherein the authentication ticket and profile information associated with the user is communicated to the second service**; and

if the second service is not associated with the first policy group identified by the stored first data:

updating the stored first data to identify the second service; and

allowing the unauthenticated user to access the second service during which the user continues to be unauthenticated for the second service **wherein authentication ticket and profile information associated with the user is <u>not</u> communicated to the second service**.

For example, the user uses the browser of client computer system to navigate to Service B, which requires the user to be authenticated because it provides personalized or premium content to the user. (Page 29, [0065]). As a result, Service B redirects the browser to an Authentication URL of central server and the Authentication URL prompts the user for his or her credentials. (Pages 29-30, [0065]). The user submits his or her credentials to central server and if the submitted credentials match an entry stored in database, then central server obtains a profile associated with the submitted credentials. (Page 30, [0066]). **Additionally, the central server may record the policy group of Service B (Policy Group P) in a "Visited Sites" cookie on the client.** (Page 30, [0066]).

Thereafter, the user navigates to a first selected service, namely, Service A which belongs to the same policy group as Service B. (Page 31, [0068]). Within Service A, there may be web pages that the service administrator would prefer but does not require the user to be authenticated in order to grant the user access to these web pages. (Page 29, [0064]). Since the user has already signed in to a site within Policy Group P, namely Service B, central server will automatically sign in the user to Service A, and an encrypted authentication ticket and profile information of the user will be communicated to Service A. (Page 29, [0064]).

Writing for the Supreme Court, Justice Anthony Kennedy observed that a patent claim is invalid for obviousness when the invention combines familiar elements according to known

methods to produce no more than predictable results. *KSR International Co. v. Teleflex, Inc.* U.S., No. 04-1350, 4/30/07. However, in this rejection, neither the **element** of **receiving a second request from the second network server to provide the second service to the user wherein authentication of the user by the second service is optional and wherein the user is not authenticated for the second service**, nor the **result** of **if the second service is not associated with the first policy group identified by the stored first data...allowing the unauthenticated user to access the second service during which the user continues to be unauthenticated for the second service** is found in the combined art.

For at least these reasons, Applicants submit that cited references, alone or in combination, do not teach or make obvious each and every element of claim 15. As such, the rejection of claim 15 under 35 U.S.C. § 103(a) should be removed. Additionally, claims 19 and 20 depending from claim 15 are allowable for at least the same reasons as claim 15. Claim 30 includes similar subject matter as claim 15 and is allowable for at least the same reasons as claim 15. Claims 32 and 34 depend from claim 30 and are allowable for at least the same reasons as claim 30.

Claim 1

receiving a first request from the first network server to provide the first service to the user wherein the user is not authenticated for the first service and not authenticated for the second service when the first request is received;

storing first data on the client in response to the received first request, said first data **identifying the first service** wherein authentication of the user by the first service is optional and wherein the user is not authenticated for the first service and not authenticated for the second service when the first data is stored;

allowing the user to access the first service without authenticating the user during which the user continues to be unauthenticated for the first service and unauthenticated for the second service **wherein the first service does not receive an authentication ticket and profile information associated with the user and wherein the user is not authenticated for the first service**;

receiving a second request from the second network server to provide the second service to the user wherein the second service requires authentication of the user, wherein the user is not authenticated for the first service and wherein the first service does not have an authentication ticket and profile information associated with the user;

authenticating the user for the second service in response to the received second request;

allowing the user access to the second service in response to authenticating the user for the second service wherein the user is not authenticated

for the first service and wherein the first service does not have an authentication ticket and profile information associated with the user;

generating, in response to authenticating the user for the second service, an authentication ticket and profile information associated with the user wherein the generated authentication ticket and profile information is communicated to the second service, wherein the user is not authenticated for the first service and wherein the first service does not have an authentication ticket and profile information associated with the user; and

authenticating in response to the authentication of the user for the second request, the user for the first service identified in the stored first data wherein, in response to the authentication of the user for the first service, the generated authentication ticket and profile information is communicated to the first service.

For example, the user navigates to a first selected service, namely, Service A, by using a browser of client computer system and within Service A there may be web pages that the service administrator would require the user to be authenticated in order to grant the user access to these web pages. (Page 19, [0045]). For example, such web pages may provide personalized content or premium content that the user has registered for and subscribed with Service A. (Page 19, [0045]). On the other hand, there may be web pages within Service A that the service administrator would prefer but does not require the user to be authenticated in order to grant the user access to these web pages. (Page 20, [0046]). For such web pages that provide "free-reach" contents, having a unique identifier for tracking the user or for serving targeted advertisements would be useful, but requiring the user to be authenticated may constitute a barrier for accessing Service A. (Page 20, [0046]). **In other words, these web pages "desire" authentication from the perspective of Service A but does not require it.** (Page 20, [0046]). Accordingly, Service A implements "soft authentication" for these web pages which allows Service A to obtain an authentication ticket and profile information f the user is already signed in to a site that shares the same set of business rules with Service A. (Page 20, [0046]).

Next, suppose the user navigates and authenticates with Service B and that Service B shares the same set of business rule (e.g. policy group) with Service A. (Page 31, [0067]). The authentication service determines that Service A wishes to authentic the user based on the first stored data. (Page 31, [0067]). In turn, Service A is notified that the user has signed in to another the same set of business rule and the user has effectively been authenticated for Service A. (Page 31, [0067]).

Writing for the Supreme Court, Justice Anthony Kennedy observed that a patent claim is invalid for obviousness when the invention combines familiar elements according to known methods to produce no more than predictable results. *KSR International Co. v. Teleflex, Inc.* U.S., No. 04-1350, 4/30/07. However, in this rejection, neither the **element** of **storing first data on the client in response to the received first request, said first data identifying the first service wherein authentication of the user by the first service is optional and wherein the user is not authenticated for the first service and not authenticated for the second service when the first data is stored** nor the **result** of **authenticating, in response to the authentication of the user for the second request, the user for the first service identified in the stored first data wherein, in response to the authentication of the user for the first service, the generated authentication ticket and profile information is communicated to the first service** is found in the combined art.

For at least these reasons, Applicants submit that cited references, alone or in combination, do not teach or make obvious each and every element of claim 1. As such, the rejection of claim 15 under 35 U.S.C. § 103(a) should be removed. Additionally, claims 2-13 depending from claim 1 are allowable for at least the same reasons as claim 1.

Claims 35-38 stand rejected under35 USC 103 (a) as being obvious over Venkataramappa in view of Stanko (U.S. Pub. App. 2005/0074126) further in view of Lutz. For the reasons stated above, Applicants submit that cited references, alone or in combination, do not teach or make obvious each and every element of claim 30 such as "**if the second policy group identified by the stored information identifying the second policy group associated with the second service is not the same as the first policy group identified by the stored first data, the central server is configured to update the stored first data to identify the second service in response to the received second request and the central server is configured to allow the unauthenticated user to access the second service during which the user continues to be unauthenticated for the second service**." As such, the rejection of claim 35 under 35 U.S.C. § 103(a) should be removed. Additionally, claims 36-38 depending from claim 35 are allowable for at least the same reasons as claim 35.

Conclusion

Applicants submit that the claims are allowable for at least the reasons set forth herein. Applicants thus respectfully submit that the claims as presented are in condition for allowance and respectfully request favorable reconsideration of this application.

Although the prior art made of record and not relied upon may be considered pertinent to the disclosure, none of these references anticipates or makes obvious the recited aspects of the invention. The fact that Applicants may not have specifically traversed any particular assertion by the Office should not be construed as indicating Applicants' agreement therewith.

Applicants wish to expedite prosecution of this application. If the Examiner deems the application to not be in condition for allowance, the Examiner is invited and encouraged to telephone the undersigned to discuss making an Examiner's amendment to place the application in condition for allowance.

The Commissioner is hereby authorized to charge any deficiency or overpayment of any required fee during the entire pendency of this application to Deposit Account No. 19-1345.

Respectfully submitted,

/Frank R. Agovino/

Frank R. Agovino, Reg. No. 27,416
SENNIGER POWERS LLP
100 North Broadway, 17th Floor
St. Louis, Missouri 63102
(314) 345-7000

FRA